

PAT-NO: JP02001306558A

DOCUMENT-IDENTIFIER: JP 2001306558 A

TITLE: METHOD AND SYSTEM FOR MANAGING
DOCUMENT

PUBN-DATE: November 2, 2001

INVENTOR-INFORMATION:

NAME	COUNTRY
KARASAWA, HIROAKI	N/A
ASHIZAWA, HIDEAKI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NTT COMMUNICATIONS KK	N/A

APPL-NO: JP2000120429

APPL-DATE: April 21, 2000

INT-CL (IPC): G06F017/21, G06F017/30 , G06F019/00

ABSTRACT:

PROBLEM TO BE SOLVED: To enable plural users to share the same document.

SOLUTION: Electronic document data composed of plural document segments and a security sheet with which a user ID is related with an access right set for each document segment, are stored on a prescribed database and when the electronic document data in the database are accessed by an arbitrary user, an ID applied from this user, who is making the access, is collated with the user ID in the database. Corresponding to this collated result, the access right

BEST AVAILABLE COPY

related to the user is retrieved from the security sheet
and corresponding to
this retrieved access right, the read or write of the
document segments is
permitted or inhibited to the user.

COPYRIGHT: (C)2001,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-306558

(P2001-306558A)

(43) 公開日 平成13年11月2日(2001.11.2)

(51) Int.Cl. ⁷	識別記号	F I	テームト [*] (参考)
G 0 6 F 17/21	5 9 6	G 0 6 F 17/21	5 9 6 A 5 B 0 0 9
17/30	1 1 0	17/30	1 1 0 C 5 B 0 7 5
	1 2 0		1 2 0 B
19/00	3 0 0	19/00	3 0 0 N

審査請求 未請求 請求項の数 9 O L (全 16 頁)

(21) 出願番号 特願2000-120429(P2000-120429)

(22) 出願日 平成12年4月21日(2000.4.21)

(71) 出願人 399035766

エヌ・ティ・ティ・コミュニケーションズ
株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 唐沢 裕明

東京都千代田区内幸町一丁目1番6号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

(74) 代理人 100064621

弁理士 山川 政樹

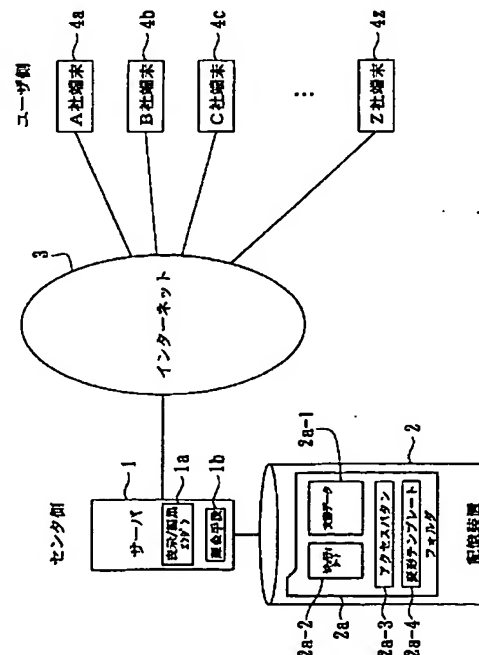
最終頁に続く

(54) 【発明の名称】 文書管理方法およびシステム

(57) 【要約】

【課題】 複数ユーザによって同一文書を共有可能とする。

【解決手段】 複数の文書セグメントからなる電子文書データと、ユーザIDと前記文書セグメント毎に設定されたアクセス権とが関連づけられたセキュリティシートとを所定のデータベースに格納し、任意ユーザによって前記データベース内の前記電子文書データがアクセスされた際に、このアクセスしたユーザから与えられたIDと前記データベース内のユーザIDとを照合し、この照合結果に応じて、前記ユーザに関連づけられているアクセス権を前記セキュリティシートから検索し、この検索されたアクセス権に応じて、前記文書セグメントの読み出しまたは書き込みを前記ユーザに許可または禁止する。



【特許請求の範囲】

【請求項1】 サプライチェーンモデルにおけるプロセス間の情報流通を電子文書にマッピングすることにより、サプライチェーン全体のコラボレーションおよびユーザ間の情報共有を実現する文書管理方法において、複数の文書セグメントからなる電子文書データと、ユーザIDと前記文書セグメント毎に設定されたアクセス権とが関連づけられたセキュリティシートとを所定のデータベースに格納し、

任意ユーザによって前記データベース内の前記電子文書データがアクセスされた際に、このアクセスしたユーザから与えられたIDと前記データベース内のユーザIDとを照合し、

この照合結果に応じて、前記ユーザに関連づけられているアクセス権を前記セキュリティシートから検索し、この検索されたアクセス権に応じて、前記文書セグメントの読み出しまたは書き込みを前記ユーザに許可または禁止することを特徴とする文書管理方法。

【請求項2】 請求項1において、前記電子文書データの表示、編集または文書処理を含む操作に対して生じる文書状態を管理することを特徴とする文書管理方法。

【請求項3】 請求項1において、前記データベースは、センタ集中型システムによって管理されていることを特徴とする文書管理方法。

【請求項4】 請求項1において、前記データベースは、ネットワーク分散型システムによって管理されていることを特徴とする文書管理方法。

【請求項5】 サプライチェーンモデルにおけるプロセス間の情報流通を電子文書にマッピングすることにより、サプライチェーン全体のコラボレーションおよびユーザ間の情報共有を実現する文書管理システムにおいて、

複数の文書セグメントからなる電子文書データと、ユーザIDと前記文書セグメント毎に設定されたアクセス権とが関連づけられたセキュリティシートとが格納されたデータベースを有する記憶手段と、

任意ユーザによって前記データベース内の前記電子文書データがアクセスされた際に、このアクセスしたユーザから与えられたIDと前記データベース内のユーザIDとを照合し、この照合結果に応じて、前記ユーザに関連づけられているアクセス権を前記セキュリティシートから検索し、この検索されたアクセス権に応じて、前記文書セグメントの読み出しまたは書き込みを前記ユーザに許可または禁止するサーバとを備えたことを特徴とする文書管理システム。

【請求項6】 請求項5において、前記サーバは、前記電子文書データの表示、編集または文書処理を含む操作に対して生じる文書状態を、さらに管理することを特徴とする文書管理システム。

【請求項7】 請求項5において、前記データベースは、センタ集中型システムによって管理されていることを特徴とする文書管理システム。

【請求項8】 請求項5において、前記データベースは、ネットワーク分散型システムによって管理されていることを特徴とする文書管理システム。

【請求項9】 請求項5において、前記サーバは、このサーバの利用料を前記ユーザから徴収するための課金手段を有することを特徴とする文書管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、文書管理方法およびシステムに関し、特に複数ユーザによって同一文書を共有可能とする文書管理方法およびシステムに関するものである。

【0002】

【従来の技術】物流、お金や情報の流れを管理することにより生産活動の最適化を図るサプライチェーンマネジメントが、アパレル業界等の各種の企業間に広まりつつある。このようなサプライチェーンマネジメントにおいては、インターネット技術を積極的に取り入れることにより、企業間または企業内の商品の企画・設計、開発、製造、見積もり、受発注、物流、決済、保守等のあらゆるプロセスの連携を図ることができ、また大規模な情報システムの構築を安価に実現できるという利点がある。また、後述のサプライチェーンモデルとは、企業間または企業内の商品の企画・設計、開発、製造、見積もり、受発注、物流、決済、保守等のあらゆるプロセスの連携（結びつき）を指すものである。

【0003】ところで、多数の異なる組織間で電子的な手法を用いて取引書類（電子メッセージ）を交換するためには、統一された規約が必要である。このような規約に基づいた電子データ交換は、一般的にEDI（Electronic Data Interchange）と呼ばれ、現在までにCII標準やEDIFACT等の種々のものが提案されている。また、EDIを用いた電子商取引においては、仕様書、企画書、発注書等の様々な文書を複数ユーザ間で交換するとともに、複数ユーザ間で同一文書を共有する場合がある。ところが、同一文書を共有しようとした場合、企業間の秘密情報が他社に漏れてしまう恐れがあるため、従来システムにおいては文書毎にアクセス権を設定し、アクセス許可の与えられたユーザのみがその文書にアクセス可能となり、内容の読み書きができるようになっていた。

【0004】

【発明が解決しようとする課題】しかしながら、このような文書アクセス権を備えた文書管理システムにおいては、ネットワーク分散型システム、センタ集中型システ

ムの何れの場合においても、システム管理者が一時的にアクセス権を設定しており、文書作成者であるユーザ自身がアクセス権を設定することはできなかった。また、一つの文書に対して一つのアクセス権が設定されており、文書中の各項目（以下、文書セグメントという）毎にアクセス権を設定することはできなかった。そのため、従来システムでは、サプライチェーン上で各ユーザが相互に文書をやり取りしたり、複数ユーザが同一文書に対して協調作業を実施したりするようなコラボレーション環境を提供することは困難であった。本発明は、この

【0005】

【課題を解決するための手段】このような目的を達成するために、本発明に係る文書管理方法は、サプライチェーンモデルにおけるプロセス間の情報流通を電子文書にマッピングすることにより、サプライチェーン全体のコラボレーションおよびユーザ間の情報共有を実現する文書管理方法において、複数の文書セグメントからなる電子文書データと、ユーザIDと前記文書セグメント毎に設定されたアクセス権とが関連づけられたセキュリティシートとを所定のデータベースに格納し、任意ユーザによって前記データベース内の前記電子文書データがアクセスされた際に、このアクセスしたユーザから与えられたIDと前記データベース内のユーザIDとを照合し、この照合結果に応じて、前記ユーザに関連づけられているアクセス権を前記セキュリティシートから検索し、この検索されたアクセス権に応じて、前記文書セグメントの読み出しまたは書き込みを前記ユーザに許可または禁

止する。
【0006】また、本発明はその他の態様として次に示す構成を含むものである。すなわち、前記電子文書データの表示、編集または文書処理を含む操作に対して生じる文書状態を管理する。また、前記データベースは、センタ集中型システムによって管理されている。また、前記データベースは、ネットワーク分散型システムによ

って管理されている。
【0007】また、発明に係る文書管理システムは、サプライチェーンモデルにおけるプロセス間の情報流通を電子文書にマッピングすることにより、サプライチェーン全体のコラボレーションおよびユーザ間の情報共有を実現する文書管理システムにおいて、複数の文書セグメントからなる電子文書データと、ユーザIDと前記文書セグメント毎に設定されたアクセス権とが関連づけられたセキュリティシートとが格納されたデータベースを有する記憶装置と、任意ユーザによって前記データベース内の前記電子文書データがアクセスされた際に、このアクセスしたユーザから与えられたIDと前記データベース内のユーザIDとを照合し、この照合結果に応じて、

前記ユーザに関連づけられているアクセス権を前記セキュリティシートから検索し、この検索されたアクセス権に応じて、前記文書セグメントの読み出しまたは書き込みを前記ユーザに許可または禁止するサーバとを備える。

【0008】また、本発明はその他の態様として次に示す構成を含むものである。すなわち、前記サーバは、前記電子文書データの表示、編集または文書処理を含む操作に対して生じる文書状態を、さらに管理する。また、前記データベースは、センタ集中型システムによって管理されている。また、前記データベースは、ネットワーク分散型システムによって管理されている。また、前記サーバは、このサーバの利用料を前記ユーザから徴収するための課金手段を有する。

【0009】したがって、このように構成することにより本発明は、文書セグメント単位、文書単位、またはフォルダ単位に対して、容易にアクセス権限を設定することができる。

【0010】

【発明の実施の形態】次に、本発明の一つの実施の形態について図を用いて説明する。図1は、本発明の一つの実施の形態を示すブロック図である。同図に示すように、本実施の形態に係る文書管理システムは、インターネット3に接続されたサーバ1と、ユーザ側の端末4a～4zとで構成されている。サーバ1はCPU等で構成された表示／編集エンジン1aおよび課金手段1b、記憶装置2を備え、この記憶装置2にはフォルダ2aが格納されている。フォルダ2aには、文書データ2a-1、セキュリティシート2a-2、セキュリティシート2a-2を構成するマスクとこのマスクを使用して作業するユーザ（ユーザID）との対応付けが登録されたアクセスボタン2a-3、文書型の変換に用いられる変形テンプレート2a-4が格納されている。なお、記憶装置2の記憶内容はデータベース化されて格納されている。また、ここではユーザ側の端末4aをA社の端末、4bをB社の端末、4cをC社の端末、4zをZ社の端末としている。表示／編集エンジン1aはユーザ側の端末4a～4zの画面表示を制御し、課金手段1bはサーバ1が提供するサービスを利用した際の各ユーザの利用料を課金する。

【0011】このように、本実施の形態ではA～Z社によって文書データ2a-2が共有され、この共有された文書データ2a-1はセンタ側の記憶装置2内に記憶保持されている。文書データ2a-1は少なくとも一以上の文書セグメントで構成され、文書セグメントは文字、記号、数字または画像データ等の集合で構成されている。文書作成にあたっては、まずサーバ1にアクセスしてフォルダ2aを作成し、作成したフォルダ2a内に所望の文書種別、文書型の文書を作成して保管する。フォルダの作成者はそのフォルダの所有者であり、したがっ

てフォルダ内に所望の文書データを作成することができるとともに、フォルダ内の全ての文書データに対してアクセス可能である。

【0012】文書種別は、ユーザから見た文書の属性であり、その具体例としては所有文書、依頼文書、公開文書、伝達文書等がある。文書作成者から見ればその文書は所有文書であり、他ユーザが作成して公開している文書であれば、それは公開文書である。また、他ユーザから読み出し/書き込み依頼されている文書は依頼文書であり、伝達された文書は伝達文書である。文書型の例としては、サプライチェーンの場合、企画書、仕様書、または発注書等がある。

【0013】一方、他ユーザによる文書データ2a-1へのアクセスは、サーバ1を介して行われる。サーバ1はアクセスしてきたユーザのIDがセキュリティシート2a-2内に登録されているか否かを検索して調べる。検索の結果、そのIDが登録されている場合は、そのユーザに設定されているアクセス条件に応じて、文書セグメント毎のアクセスを許可し、読み出しや書き込みを可能とする。この読み出しおよび書き込み処理は、サーバ1内の表示/編集エンジン1aによって行われる。すなわち、表示/編集エンジン1aが、セキュリティシート2a-2に登録されているアクセス権に応じてユーザ端末上に文書を表示させたり、書き込みを受け付けたりする。

【0014】セキュリティシート2a-2は、文書データ2a-1の作成者によって作成され、文書セグメント単位でアクセス権が設定されている。したがって、あるユーザがサーバ1にアクセスして文書一覧を表示させた場合、セキュリティシート2a-2にそのユーザが登録されていなければ、文書一覧中にはその文書名さえも表示されず、またアクセス権が設定されていたとしても、許可された文書セグメントについてのみしか読み出しまたは書き込みはできない。

【0015】図2は、ユーザ側端末の表示例を示す平面図である。ユーザ側の端末には同図に示す画面表示がされ、表示された各種のボタンを操作することにより、文書データの編集や画面表示の制御等を行うことができる。サービスボタン101は、ユーザに対して各種のサービス(文書編集、他ユーザに対する文書の読み出し依頼/書き込み依頼、伝達等)を提供するためのボタンである。すなわち、図示しないマウス・ポインタ等の入力装置によってクリックされるとドロップダウン・メニュー(図示せず)が表示される。そこで、ドロップダウン・メニュー内に表示された各種のサービス(ボタン)を、さらにマウス・ポインタでクリックすることにより、所望のサービスを選択して実行することができる。

【0016】また、ログアウトボタン102は、現在実行中のサービスを終了するためのボタンである。フォルダ選択ボタン103は、アクセス可能なフォルダの表示

および選択するためのボタンである。確定/確定解除ボタン104は、編集した文書の確定指示の入力、または確定されている文書の確定解除を入力するためのボタンである。なお、文書種別によっては、確定/確定解除ボタン104の代わりに報告ボタン105が表示される。すなわち、所有文書の場合は確定/確定解除ボタン104が表示され、依頼文書および伝達文書の場合は報告ボタン105が表示される。

【0017】このようにフォルダ選択ボタン103をクリックした後、所望のフォルダを選択することにより、そのフォルダ内に格納されている文書データの一覧が表示される。マウス・ポインタを使って所望の文書を選択すると、画面中央部にその文書が表示される。表示された文書の上方には、フォルダ名、文書名、文書作成者名、会社名、文書型、文書種別、フォルダ種別、文書状態等の各種の情報が表示される。ユーザはセキュリティシートに設定されているアクセス権に応じて、その文書を編集することができ、編集後に確定ボタンをクリックすれば、以降の編集操作はできなくなる。再度編集したい場合は、確定解除ボタンをクリックすることによって確定状態を解除する必要がある。

【0018】図3は、セキュリティシートを説明するための説明図である。ユーザは文書データを作成するとともに、セキュリティシートを設定することによって、その文書に対する他ユーザのアクセス権を設定することができる。例えば同図(a)に示すように、セキュリティシートを設定することにより、文書中の所望の文書セグメントのみをA社に対してアクセス可能にすることができる。また、同図(b)に示すように文書全体をアクセスできるようにしてもよい。さらに、同図(c)に示すように、A社に対してフォルダ内の全ての文書のアクセスを許可することもできる。

【0019】ここで、セキュリティシートについて説明する。図4は、セキュリティシートを示す模式図である。同図に示すように、セキュリティシートは、ユーザ(ユーザID)毎(A社~Z社)に設定された、複数のマスクによって構成されている。したがって、文書作成者はユーザ毎にマスクを設定することにより、作成した文書に対するアクセス権を設定することができる。

【0020】図5は、マスクを示す模式図である。同図に示すように、マスクは文書セグメント毎に対応付けられたアクセス権に関する情報で構成されている。文書セグメントは一つの文書の内容単位を示し、アクセス権はアクセスしてきたユーザがそのセグメントの読み出しまたは書き込みの何れができるかを記載している。例えばRW(読み書き可能)であれば読み出しおよび書き込みの両方を実施することができる。RO(読み出し専用)であれば読み出しのみを実施することができる。また、アクセス権が設定されていない場合は、その文書はアクセスしたユーザの端末に表示されず、したがって読み出

しおよび書き込みの両方共に実施することができない。

【0021】図6は、XML (Extensible Markup Language) で記載されたセキュリティシートの具体例を示す。同図においては、A社とB社についてのマスクが設定され、これらの会社に対するアクセス権が記載されている。各マスクにはマスク名(<maskname>)、タイプ(<type>)、マスク設定(<maskdefine>)等が設定されている。マスク名は各マスクを一意に識別するための名前であり、この例では「マスクfor A社」と「マスクfor B社」の2つのマスクが記載されている。タイプはそのマスクが読み出し専用(RO)、読み書き可能(RW)の何れかを設定するための識別子である。また、各文書セグメントは「生地会社名」、「生地品名」、「生地品番」といったXMLのタグと対応しており、これらのタグに上述のRO、RWを設定することで読み出し/書き込み許可が設定される。なお、タイプ(<type>)が設定されていない場合は、その文書セグメントはユーザ端末に表示されず、したがって読み出しおよび書き込みの何れともできない。

【0022】まず、A社について説明する。タイプ(<type>)がROとなっていることから、A社に対しては読み出しのみが設定されている。また、「生成者部課名」、「生成日付」、「生地会社名」、「生地品名」、「生地品番」等の文書セグメントもROが設定されている。次にB社については、タイプ(<type>)がRW(読み書き可能)が設定されている。文書セグメントに関しては、「生成者部課名」、「生成日付」、「ボタン会社名」についてはRO(読み出し専用)が設定されているが、「ボタン品名」や「ボタン品番」等の文書セグメントについてはRW(読み書き可能)が設定されている。これらの設定事項は、サーバ1の表示/編集エンジン1aによって読みとられるとともに、ユーザに対する読み出し/書き込みの制御が行われる。

【0023】ここで、セキュリティシートを使った読み出し処理および書き込み処理の詳細について図を参照しながら説明する。図7は、セキュリティシートによる読み出し処理を説明するためのフローチャートである。以下においては図1のA社による読み出し処理について例示する。まず、図1のA社(端末4a)から記憶装置2内の文書データに対するアクセスがあった後、表示/編集エンジン1aは図5のテーブル(実際には図6のセキュリティシート)に登録されているタグ(文書セグメント)を一つ選択し(ステップ101)、このタグを読み出し対象となっている文書データの上から走査する(ステップ102)。その際に、A社に対して読み出し許可の与えられているタグを見つけると、そのタグを抽出する(ステップ103)。

【0024】以上のステップ101~103を図5中の全てのタグについて行ってから(ステップ104)、抽出されたタグをマージして読み出し許可の与えられてい

るタグのサブセットを作成する(ステップ105)。その後、表示/編集エンジン1aは、この作成されたサブセットをA社の端末4aに送信し(ステップ106)、端末4aにおいては受信したサブセットがユーザの操作等に応じて画面表示される(ステップ107)。この結果、読み出し許可の与えられているタグのみが端末4aに表示される。上記処理方法では、読み出し許可の与えられていない文書セグメントを一切ユーザ端末に送信しないため、ユーザ端末で表示/非表示を制御する場合に比べてセキュリティ上優れている。

【0025】図8は、セキュリティシートによる書き込み処理を説明するためのフローチャートである。ここでは図1のA社による書き込み処理について例示する。まず、図1のA社により、端末に表示されている読み出し可能タグが編集されてから(ステップ201)、端末4aに表示されている保存ボタンがクリックされると、この保存されたサブセットはサーバ1へ送信され(ステップ202)、サーバ1においては受信したサブセットを図1の記憶装置2に保存する(ステップ203)。

【0026】表示/編集エンジン1aは、図5のテーブル(実際には図6のセキュリティシート)に登録されているタグを一つ選択し(ステップ204)、この選択されたタグをステップ203で保存されたサブセットの上から走査し(ステップ205)、書き込み許可の与えられている全てのタグを検出すると(ステップ206)、サーバ1上の元の文書データにこの検出された全てのタグを、元の文書データの対応する位置に書き戻す(ステップ207)。以上のステップ204~207をサブセット中の全てのタグを走査するまで行う(ステップ208)。この結果、A社による編集内容(ただし、書き込み許可の与えられたタグのみ)は、記憶装置2内の元の文書データに反映される。

【0027】以上のように、セキュリティシートを設定することによって、文書に対する他ユーザのアクセス権を容易に設定することができるが、図6に示したようなマスクを一々記載したのでは手間がかかるため、予めアクセスボタンとして用意しておけば便利である。図9はアクセスボタンを示す模式図である。同図に示すように、セキュリティシートに記載されているマスクは、ユーザ(ユーザID)毎に固有のものである。そのため、これらのマスクをアクセスボタンとして用意しておけば、その他の文書を作成した場合に、アクセスボタンに記載されているマスクをコピーするだけで済み、一々マスクを作成し直す手間を省くことができる。また、マスクは、書き込み依頼に用いるマスク、読み出し依頼に用いるマスク、伝達に用いるマスクをそれぞれ個別に用意しておけばより使いやすいものとなる。

【0028】次に、文書状態について説明する。ユーザによって作成された文書に各種の状態を設定すると、文書を管理する上で種々の利点が得られる。図10は、文

10

20

30

40

50

書状態を説明するための状態遷移図である。同図に示すように、文書が作成されていない時点では文書は不存在の状態であり、作成されることにより未確定状態に移行する。この状態は文書の編集を意味し、文書の所有者または所有者によって編集許可の与えられている者であれば、継続して文書の編集を実施することができる。その後、文書が完成したのであれば、確定ボタンのクリックによって確定状態に移行し、文書編集が不可能な状態となる。ただし、確定を解除すれば、再び未確定状態となって文書編集が可能となる。また、確定した状態で文書を削除すれば文書不存在の状態へ移行する。

【0029】一方、未確定状態において、書き込みまたは読み出し依頼を任意ユーザに出した場合、未確定状態（書込／読出依頼中）へ移行する。依頼先の端末にはこの依頼文書が表示可能となる。その後、依頼主によって上記依頼が解除されたり、依頼文書の読み出し／書き込みを行った任意ユーザが依頼主に対して終了報告を送信したりすると、再び文書状態は未確定状態（編集集中）となる。このとき任意ユーザの端末からは、上記依頼文書の表示は消える。このように文書状態は、文書データの表示、編集または文書処理を含む操作によって切り替わる。

【0030】次に、文書型の変換について説明する。ある文書型（例えば「企画書」）を他の文書型（例えば「仕様書」）へ変換するためには変形テンプレートを用いる。図11は、変形テンプレートを説明するための説明図である。ユーザによって作成された文書は、サーバ1内の表示／編集エンジン1aが変形テンプレートを実行することにより、その他の文書型の文書に容易に変換することができる。同図（a）に示すように、変形テンプレートを実行することにより、企画書を仕様書に変換することができる。また、同図（b）に示すように、一つの仕様書から複数の発注書を作成することもできる。さらに、同図（c）に示すように、複数の仕様書から一つの発注書を作成することもできる。

【0031】このような文書データの変換は、ユーザによる意識的な操作によって実施されてもよいし、表示、編集または文書処理を含む操作によって生じる文書状態の切り替わりをトリガとして実施されてもよい。すなわち、あるユーザが仕様書の書き込み依頼を受けた場合、仕様書に所定事項を記入した後上述の確定ボタンをクリックすることにより、依頼主に報告が通知されるとともに、仕様書および変形テンプレートに基づいて発注書が作られる。なお、変換前の文書型と変換後の文書型の組み合わせは以上に限られるものではなく、適宜組み合わせることができる。

【0032】図12は、XMLで記載された変形テンプレートの一例を示す説明図である。同図において、タイプ（<type>）は変形テンプレートの使用タイプを示す。使用タイプとしては分解（元の文書データを一以上の文

書データに変換）、新規（新規の文書型のデータを作成）、新規／既存（分解、新規文書データの作成、既存文書データの更新）、既存（既存の文書データに反映）がある。文書型（<from-DTD>,<to-DTD>）は変換前（from側）の文書型、変換後（to側）の文書型をそれぞれ指定するための識別子である。ここではfrom側の文書型は「企画書」であり、to側の文書型は「仕様書」である。【0033】この例では転記に関係のないto側のタグ「仕様書番号」、「素材受注者」、「素材発注日」、「素材品番」、「素材着荷指定日」、「素材出荷先」、「縫製受注者」、「縫製発注日」、「縫製着荷指定日」、「縫製詳細」および「縫製数量」は、from側で省略されている。これらのタグに関しては変換後の「仕様書」においてタグのみが記載され、その中身は空欄となる。また、「*a001」や「*a102」等の識別子で指定されているタグについては、タグの中身も「仕様書」に反映される。例えば「企画書」の「鹿島アパレル」、「ポリエステル」、「2000」等は「仕様書」に転記される。

【0034】図13は、アパレル関係のサプライチェーンに適用した場合の変形テンプレートの駆動例を示す説明図である。同図に示すように、XMLで記載された企画書には「発注者」として「鹿島アパレル」が記載されている。また、3つの文書セグメント（素材関連）があり、1番目の文書セグメントには「素材名」として「ポリエステル」、「素材数量」として「2000」が記載され、2番目の文書セグメントには「素材名」として「ウール」、「素材数量」として「1000」が記載され、3番目の文書セグメントには「素材名」として「カシミア」が記載され、「素材数量」として「3000」が記載されている。これを変形テンプレートの実行により仕様書に変換すると「仕様書番号」のタグが追加されるとともに、文書セグメント（素材関連）内に「素材発注者」、「素材発注日」、「素材品番」、「素材着荷指定日」および「素材出荷先」のタグが追加される。また、「素材関連」のタグの下には、「縫製受注者」、「縫製発注日」、「縫製着荷指定日」、「縫製詳細」および「縫製数量」のタグが追加される。空欄のタグの中身は書き込み依頼先のユーザ等によって記載される。

【0035】また、図12の変形テンプレートでは「素材関連」のタグを1回しか記載していないが、「企画書」に複数の「素材関連」のタグが記載されているときは、同様の変換を複数回繰り返すことになる。すなわち、図13（a）の「企画書」には3個の「素材関連」のタグ（ポリエステル、ウール、カシミア）が記載されているため、変形テンプレートの実行時には、各「素材関連」のタグに対して「素材受注者」等のタグの追加および「素材名」の転記等が行われ、3個の「素材関連」のタグが生成される。したがって、変形テンプレートにおいては、同一タグの変換を冗長して記載する必要がな

い。

【0036】ここで、変形テンプレートの駆動について図を参照しながら詳細に説明する。図14は、変形テンプレートの駆動を説明するためのフローチャートである。まず、図1の表示／編集エンジン1aは、ステップ301において、変形テンプレート中のfromタグの記述と、実際のfrom型の文書（図11では企画書）とのパターンマッチングを行う。次いで、ステップ302、303において、各タグの繰り返し登場回数を記録し（図11では素材関連のタグは3回、その他のタグは1回）、この繰り返し登場回数を考慮して変形テンプレート中のto型の文書を新規に作成する（図11では素材関連のタグを3回記載し、その他のタグを1回記載する）。

【0037】次いで、ステップ304、305において、変形テンプレート中のtoタグの記述と、新規に作成された文書とのパターンマッチングを行い、識別子「*axxx」を有するタグに関しては、「*axxx」に相当する記述をfrom型の文書から新規に作成されたto型の文書に転記する。以上のステップ301～305を全ての識別子「*axxx」について行うことにより、全ての転記が行われる。なお、図11では「*a001」に関して1回の転記（「鹿島アパレル」）が行われ、「*a102」に関して3回の転記（「ポリエステル」、「ウール」、「カシミア」）が行われ、「*a103」に関して3回の転記（「2000」、「1000」、「3000」）が行われる。

【0038】次に、本実施の形態を分散型のシステムに適用した場合について説明する。上記においては、文書管理を行うサーバが1台のセンタ集中型システムについて説明したが、文書データを管理するサーバが複数あるようなシステム（分散型システム）についても、本発明を適用することができる。図15は、分散型システムをネットワーク構成図である。インターネットに接続された複数のサーバ10、11、12と、インターネットに接続されたユーザ側の端末4a、4b、4c、・・・、4zとで構成されている。各ユーザの管理するフォルダはネットワーク上の各所に点在し、サーバ10～12が協調して管理することにより、図1で示した文書管理を実現することができる。

【0039】なお、各サーバはサーバの利用料を徴収するための手段を備え、変形テンプレートの使用数や格納されている文書の容量等に基づく従量制の課金を各ユーザに対して行うことができる。もちろん、利用時間や利用文書容量に関わらず、定額制の課金を課すようにしてもよい。また、このような課金は、センタ集中型システム、分散型システムの何れにおいても適用できる。

【0040】図16は、本発明を適用したサプライチェーンモデルの全体構成（XMLハンドリングモデル）を示す説明図である。生産、在庫、購買、販売、物流等の

情報をリアルタイムで交換することでチェーン全体の効率を向上させるサプライチェーン・マネジメントにおいては、プロセス間の情報流通をドキュメントにマッピングすることにより（プロセス・マッピング）、サプライチェーン全体のコラボレーションおよびユーザ間の情報共有を実現する。そこで、図2～14で説明した要素技術を図1、15で説明した全体構成に適用することにより、従来にない優れたサプライチェーンを実現することができる。

10 【0041】図16に示すように、文書管理を行うサーバ内には、文書作成テンプレートに従って作成されたXML文書が格納されている。各ユーザはサーバにアクセスすることにより、このサーバ内に格納されているXML文書を読み出して表示させたり、編集および作成を行ったりすることができる。文書データの表示処理は表示テンプレートの実行により行われ、文書データの編集および作成処理は編集テンプレートの実行により行われる。また、サーバ内に格納されているXML文書は、図3で説明した読み出し用のセキュリティシート（読出セキュリティマスク）や書き込み用のセキュリティシート（書込セキュリティマスク）に記載されている許可情報に基づいて、各ユーザに対して読み出し／書き込みが許可される。すなわち、各ユーザはこの許可情報で規定された範囲（参照可能範囲）についてのみアクセスすることができる。なお、表示テンプレート、編集テンプレートおよび文書作成テンプレートは、何れもセキュリティシート等と同様にXMLで記載されたテンプレートであり、図2で示したのと同様の画面をユーザ端末に表示させ、文書の表示処理、編集処理および文書作成処理を支援する。

【0042】また、サーバ内のXML文書は、図11で説明した変形テンプレートに従って複数の文書に分解されたり、内容が更新されたりする。さらに、ユーザが所有するXMLファイルをサーバにアップロードすることにより、サーバ内に新規文書を登録したり、既に登録されているXML文書の内容を更新させたりすることもできる。

【0043】

40 【発明の効果】以上説明したとおり本発明は、複数の文書セグメントからなる電子文書データと、ユーザIDと前記文書セグメント毎に設定されたアクセス権とが関連づけられたセキュリティシートとを所定のデータベースに格納し、任意ユーザによって前記データベース内の前記電子文書データがアクセスされた際に、このアクセスしたユーザから与えられたIDと前記データベース内のユーザIDとを照合し、この照合結果に応じて、前記ユーザに関連づけられているアクセス権を前記セキュリティシートから検索し、この検索されたアクセス権に応じて、前記文書セグメントの読み出しまたは書き込みを前記ユーザに許可または禁止する。

【0044】したがって、このように構成することにより本発明は、エンドユーザに文書のアクセス権を設定させ、ユーザが管理主体となっている文書に対して文書内容によるアクセス権限まで定義させることにより、一つの文書で排他制御することなく容易に協調作業環境を作り出すことができる効果がある。また、表示、編集、文書処理を含む操作に対して生じる文書状態を自動遷移させ、その契機によって文書管理を行うことにより、サプライチェーン上での文書処理と状態遷移とを連鎖的に行うことを可能とする効果がある。

【図面の簡単な説明】

【図1】 本発明の一つの実施の形態を示すネットワーク構成図である。

【図2】 ユーザ側端末の表示例を示す平面図である。

【図3】 セキュリティシートを説明するための説明図である。

【図4】 セキュリティシートを示す模式図である。

【図5】 マスクを示す模式図である。

【図6】 セキュリティシートの具体例を示す説明図である。

【図7】 セキュリティシートによる読み出し処理を説明するためのフローチャートである。

【図8】 セキュリティシートによる書き込み処理を説明するためのフローチャートである。

【図9】 アクセスボタンを示す模式図である。

【図10】 文書状態を説明するための状態遷移図である。

【図11】 変形テンプレートを説明するための説明図である。

【図12】 変形テンプレートの具体例を示す説明図である。

【図13】 アバレル関係のサプライチェーンに適用した場合の変形テンプレートの駆動例を示す説明図である。

【図14】 変形テンプレートの駆動を説明するためのフローチャートである。

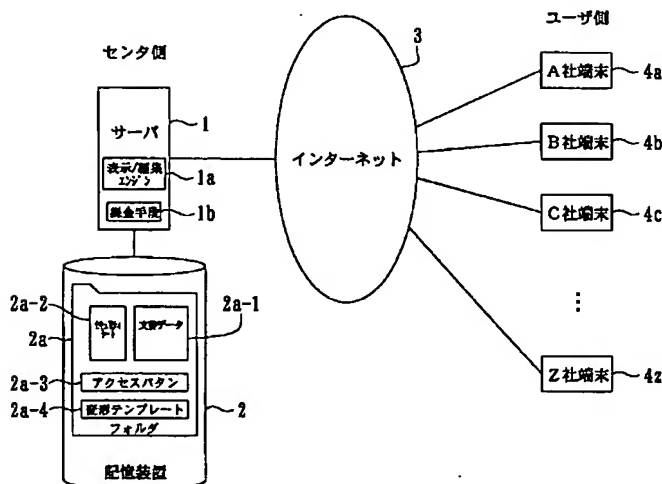
【図15】 分散型システムをネットワーク構成図である。

【図16】 本発明を適用したサプライチェーンモデルの全体構成（XMLハンドリングモデル）を示す説明図である。

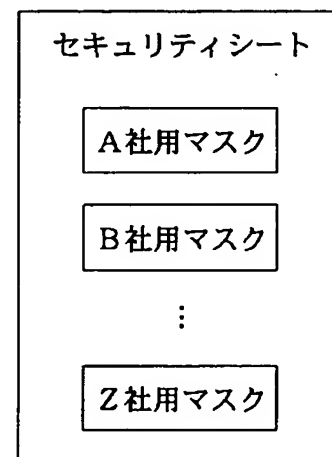
【符号の説明】

1…サーバ、1a…表示/編集エンジン、1b…課金手段、2…記憶装置、2a…フォルダ、2a-1…文書データ、2a-2…アクセスボタン、2a-3…セキュリティシート、2a-4…アクセスボタン、2a-4…変形テンプレート、3…インターネット、4a…ユーザ側端末、4b…ユーザ側端末、4c…ユーザ側端末、4z…ユーザ側端末。

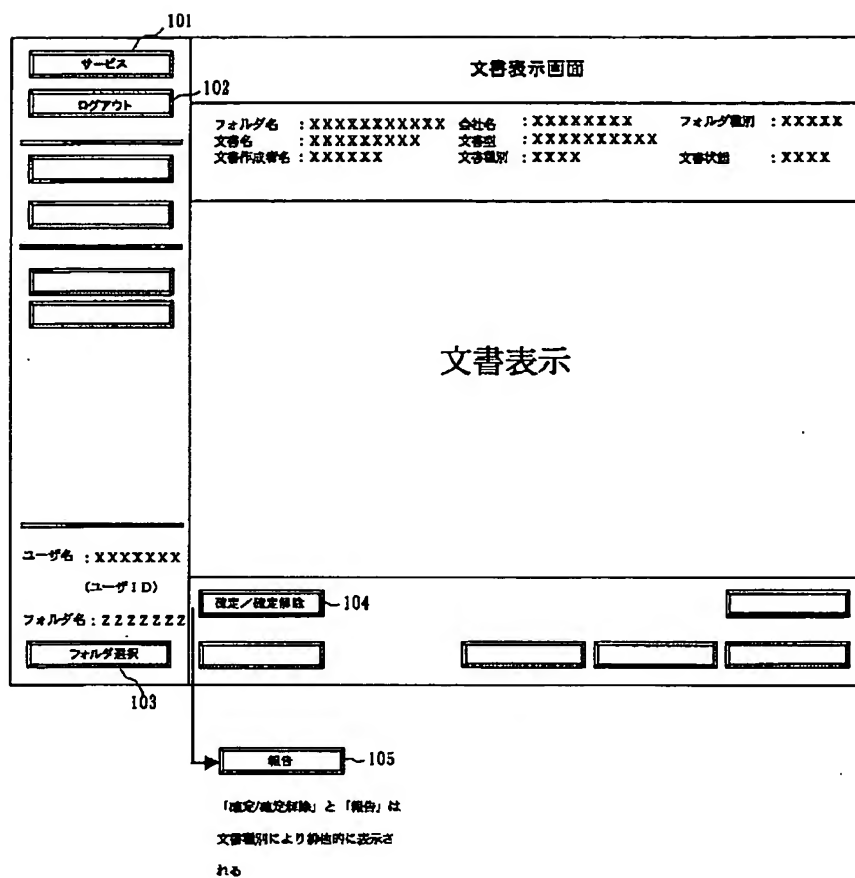
【図1】



【図4】



【図2】



【図5】

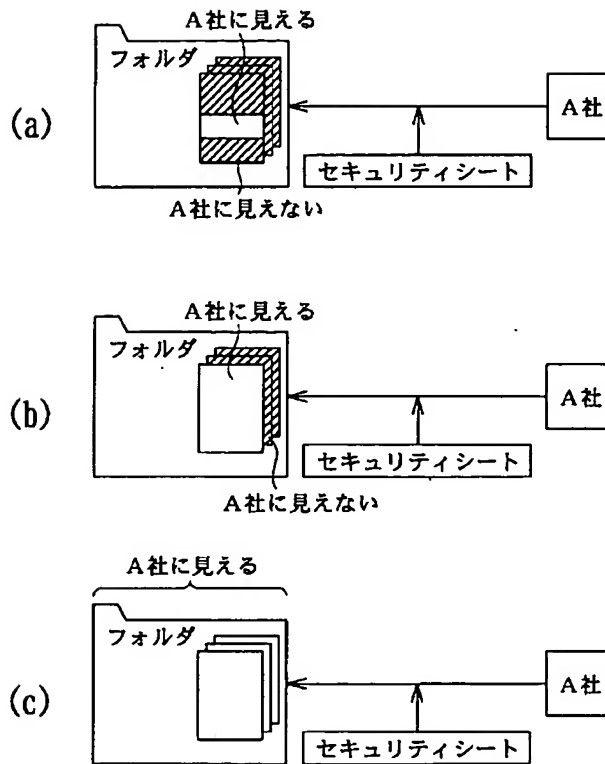
マスク	
文書セグメント	アクセス権
1	RW
2	—
...	...
N	RO

→ 読み書き可能

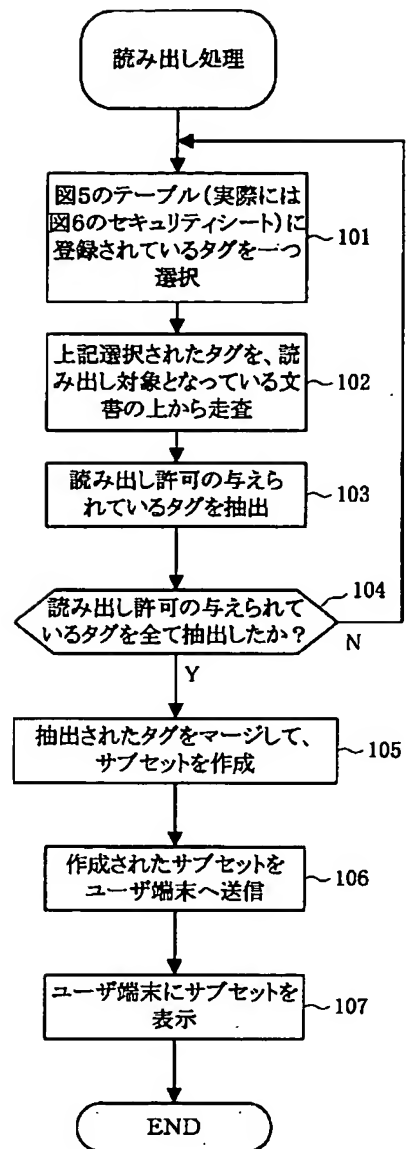
→ アクセス不可

→ 読み出し専用

【図3】



【図7】



【図6】

```

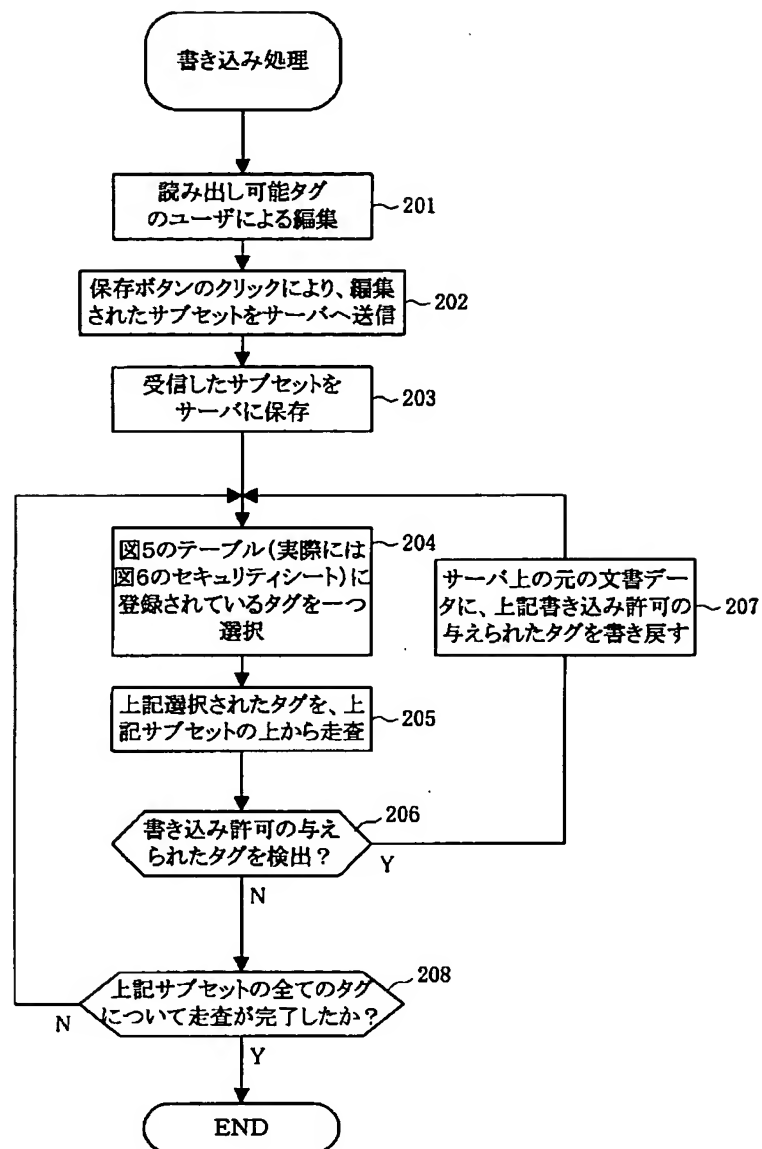
<?xml version="1.0" encoding="Shift_JIS"?>
<!--セキュリティシート例 -->
<secure>
  <define>
    <maskname> マスク for A 社</maskname>
    <type>RO</type>
    <maskdefine>
      <ApparelARC>
        <作成者部課名> RO</作成者部課名>
        <作成日付> RO</作成日付>
        <生地情報>
          <生地会社名>ScopeX,M(%OPERATOR_CORP_NAME%)</ 生地会社名>
          <生地品名> RO,ScopeX</ 生地品名>
          <生地品番> RO,ScopeX</ 生地品番>
        </生地情報>
      </ApparelARC>
    </maskdefine>
  </define>
  <define>
    <maskname> マスク for B 社</maskname>
    <type>RW</type>
    <maskdefine>
      <ApparelARC>
        <作成者部課名> RO</作成者部課名>
        <作成日付> RO</作成日付>
        <ボタン情報>
          <ボタン会社名>RO,ScopeY,M(%OPERATOR_CORP_NAME%)</ ボタン会社名>
          <ボタン品名>RW,ScopeY</ ボタン品名>
          <ボタン品番>RW,ScopeY</ ボタン品番>
        </ボタン情報>
      </ApparelARC>
    </maskdefine>
  </define>
</secure>

```

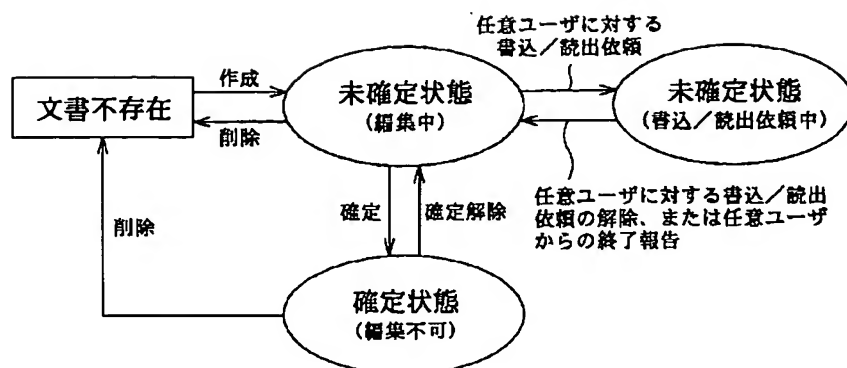
【図9】

アクセスパターン			
ユーザ名	書き込み依頼 マスク	読み出し依頼 マスク	伝達 マスク
A 社	マスクA1	マスクA2	マスクA3
B 社	マスクB1	マスクB2	マスクB3
⋮	⋮	⋮	⋮
Z 社	マスクZ1	マスクZ2	マスクZ3

【図8】



【図10】

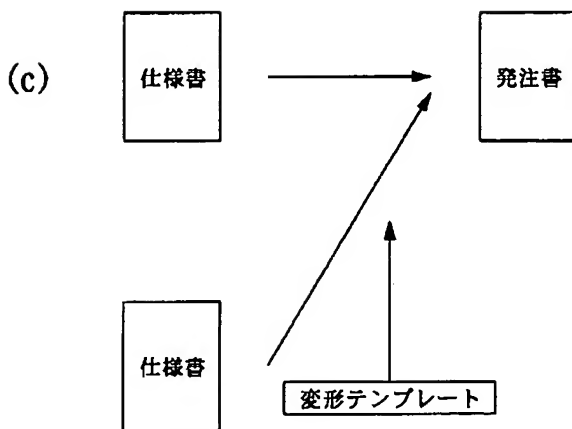
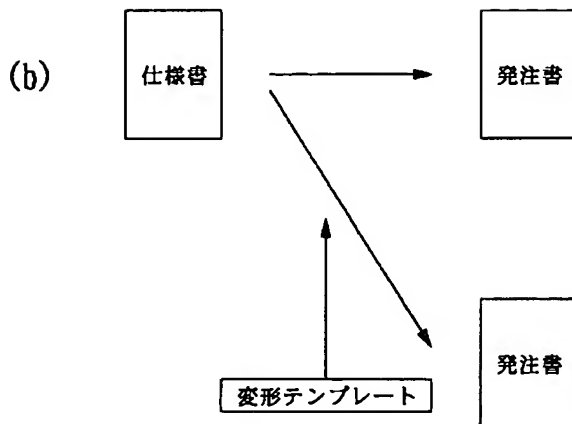
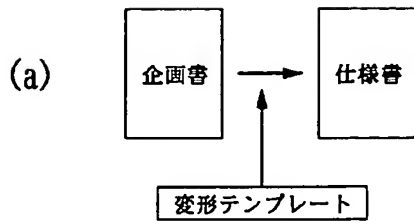


【図12】

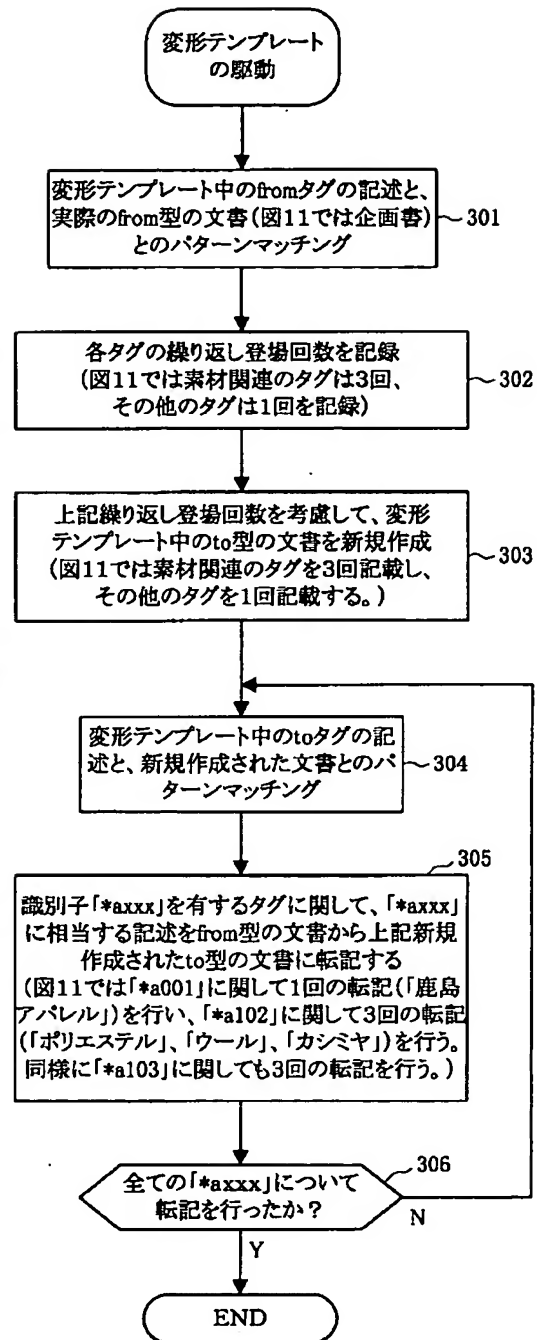
```

<?xml version="1.0" encoding="Shift_JIS"?>
<!--変形テンプレート：新規の例-->
<transform>
  <type>新規</type>
  <from-DTD>企画書</from-DTD>
  <to-DTD>仕様書</to-DTD>
  <search/>
  <section name="S01">
    <from>
      <企画書>
        <発注者>*a001</発注者>
        <素材関連>
          <素材名>*a102</素材名>
          <素材数量>*a103</素材数量>
        </素材関連>
      </企画書>
    </from>
    <to>
      <仕様書>
        <仕様書番号/>
        <発注者>*a001</発注者>
        <素材関連>
          <素材受注者/>
          <素材発注日/>
          <素材品番/>
          <素材名>*a102</素材名>
          <素材数量>*a103</素材数量>
          <素材着荷指定日/>
          <素材出荷先/>
        </素材関連>
        <縫製受注者/>
        <縫製発注日/>
        <縫製着荷指定日/>
        <縫製詳細/>
        <縫製数量/>
      </仕様書>
    </to>
  </section>
</transform>
  
```

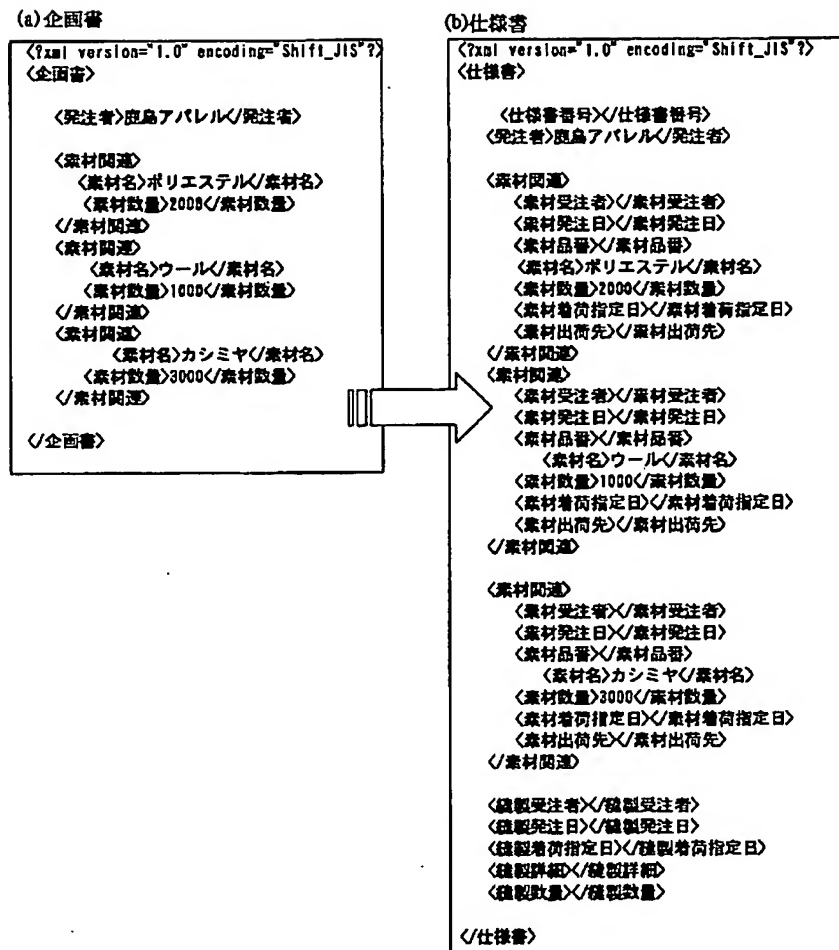
【図11】



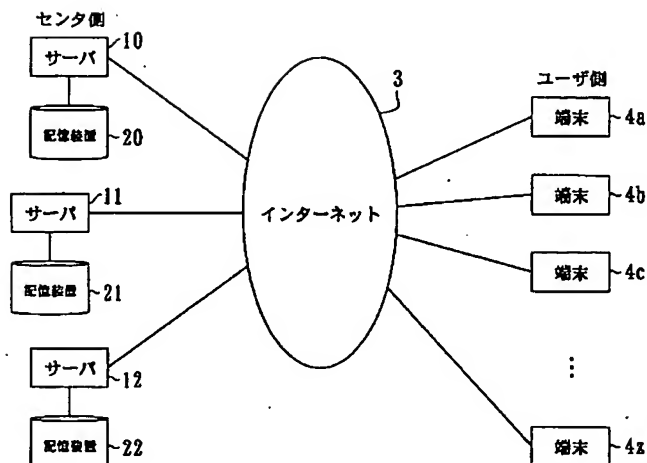
【図14】



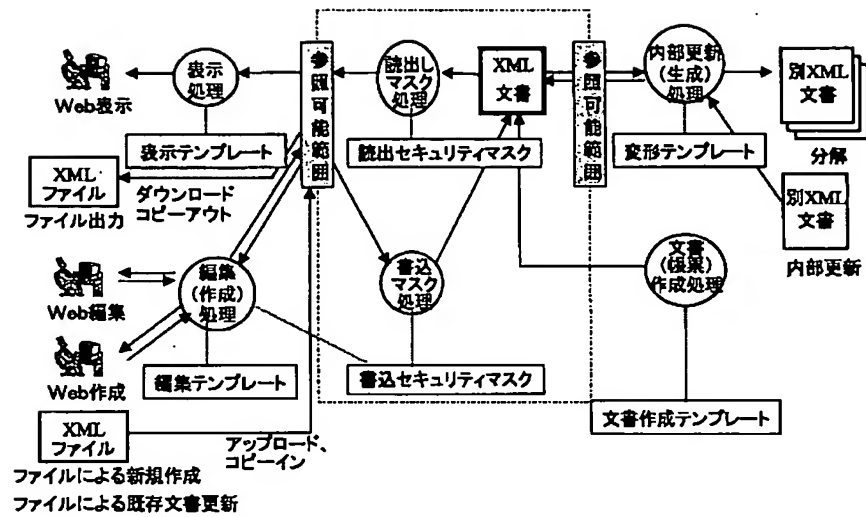
【図13】



【図15】



【図16】



フロントページの続き

(72)発明者 芦沢 秀明
 東京都千代田区内幸町一丁目1番6号 エ
 ヌ・ティ・ティ・コミュニケーションズ株
 式会社内

Fターム(参考) 5B009 VC03
 5B075 KK02 KK07 KK43 KK54 KK62
 KK64 KK65 ND03

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☐ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.